IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA, v. MAKSIM BOIKO a/k/a Maxim Boyko a/k/a "gangass"	Magistrate No. 20-658M **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Special Agent Samantha Shelnick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since March 2016. As an agent of the FBI, your Affiant has received training and gained experience in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of financial and computer-related evidence. I am currently assigned to the FBI's Pittsburgh Field Office. I have experience in the investigation of computer intrusion and computer-related financial fraud, including those activities involving violations of Title 18, United States Code, Section 1956(h) (Conspiracy to Commit Money Laundering).

2. The information contained in this affidavit is based upon my personal knowledge, knowledge obtained during my participation in this investigation, knowledge obtained from other individuals, including my conversations with other law enforcement officers, knowledge obtained from my review of documents, computer records, and other evidence related to this investigation, and knowledge gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect

of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause.

3. This Affidavit is submitted in support of an application for a criminal complaint and arrest warrant for Maksim BOIKO (BOIKO). As set forth herein, there exists probable cause to believe that from in or around 2015, the exact date being unknown, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendant Maksim BOIKO did knowingly and intentionally conspire and agree with other persons known and unknown, to commit money laundering in violation of Title 18, United States Code, Section 1956(h), that is:

a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, involving the proceeds of specified unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, wire fraud, in violation of Title 18, United States Code, Section 1343, and bank fraud, in violation of Title 18, United States Code, Section 1344, knowing that the transactions were designed, in whole and in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transactions knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

b. to knowingly transport, transmit, transfer, and attempt to transport, transmit, and transfer monetary instruments and funds from a place in the United States to and through a place outside the United States, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represent the proceeds of some form of unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, wire fraud, in violation of Title 18, United States Code, Section 1343, and bank fraud, in violation of Title 18, United States Code, Section 1344, and knowing that such transportation, transmission, and transfer was designed, in whole and in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of the specified unlawful activity, contrary to the provisions of Title 18, United States Code, Section 1956(a)(2)(B)(i).

PROBABLE CAUSE

4. Maksim Boiko, aka Maxim Boyko, aka gangass, is a 29-year-old Russian National who entered the United States via Miami, Florida with his wife on January 19, 2020.

5. Because he entered the country with $20,000 in U.S. currency, Boiko was interviewed by U.S. Customs and Border Protection. In the interview, Boiko stated that his income came from investments in Bitcoin and rental properties in Russia.

6. As explained below, the FBI has probable cause to believe that, contrary to these assertions, Boiko is a significant cybercriminal who launders money for other cybercriminals through: (1) providing other cybercriminals with access to criminally controlled bank accounts for the purpose of receiving and laundering funds stolen from victims' online bank accounts; and (2) converting criminally-derived funds from fiat currency into electronic currency, such as Bitcoin.

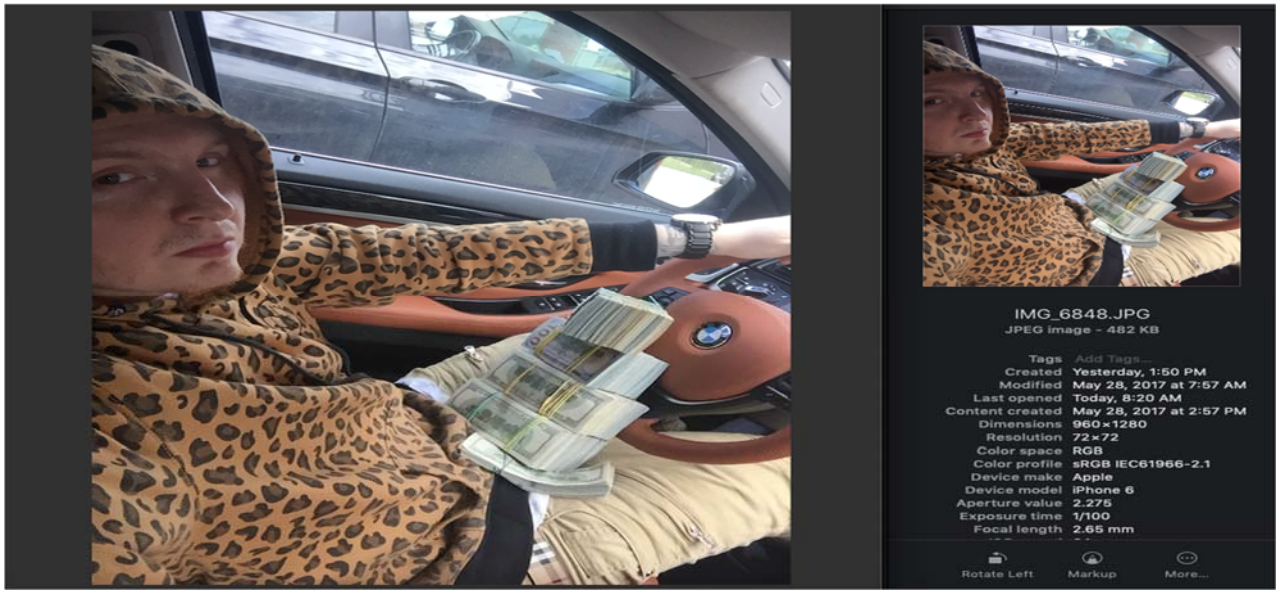
Evidence of Unexplained Wealth

7. In addition to entering the U.S. with $20,000 in U.S. currency on January 19, 2020, Boiko's Instagram social media and Apple iCloud accounts include photographs of him with substantial sums of U.S. and foreign currencies dating back as far as 2015. The photographs immediately below, which are evidence of Boiko's unexplained wealth, are inconsistent with the practices of a legitimate business operation and are consistent with the allegations set forth herein that Boiko has engaged in illegal money laundering activities with significant cybercriminals for the past several years. Immediately below is a photograph of Boiko (identified by his distinct arm tattoos) holding a large sum of U.S. currency that was posted to Boiko's Instagram account on May 13, 2017.

Immediately below is a photograph of Boiko that was posted to his Instagram account on March 24, 2016.

Immediately below is a photograph of Boiko posted to his Instagram account on December 17, 2015.

Immediately below is a photograph of Boiko taken on May 28, 2017 that was discovered in a court-authorized search of Boiko's Apple iCloud account.



Immediately below is a photograph taken on May 14, 2019, that was discovered in a court-authorized search of Boiko's Apple iCloud account.

8. Additionally, as explained below, there is probable cause to believe that Boiko laundered some of the stolen funds through bank accounts in China. This is consistent with the photograph immediately below that was posted to Boiko's Instagram account on August 25, 2015, and shows a large stack of Chinese Yuan on a table along with a sign that says "Maksim" and the date of "25 08 2015."

Background Information Concerning Boiko's Use of the Online Moniker "Gangass" in Furtherance of Criminal Activity

9. To hide his true identity, Boiko sometimes used an online moniker known as "Gangass" in furtherance of his criminal activities. To conceal communications with his cybercriminal clientele, he utilized secure and encrypted Jabber instant message platforms, to include "exploit.im" used almost exclusively by cybercriminals.

10. A search of FBI databases revealed that the email account plinofficial@me.com was used to register an account on BTC-e. BTC-e was a virtual currency exchange website that was seized by law enforcement in 2017 in connection with the website's involvement in the exchange of criminally-derived funds. The registrant using this email provided the name "Maksim Boiko" and the username "gangass." The data from BTC-e showed that Boiko's account had received $387,964 worth of deposits and had withdrawn approximately 136 Bitcoin.

11. As explained in greater detail below, a screenshot sent between Boiko's phone (ending in 0504) and a phone (ending in 2576) used by one of Boiko's cybercriminal clients

showed a login to a website with the username "gangass," which is the identical name used by Boiko to register for BTC-e.

12. A review of FBI holdings also revealed Jabber chats involving criminal money laundering committed by an individual using the Jabber account gangass@exploit.im. For the reasons explained below, there is probable cause to believe that gangass@exploit.im is Boiko. Further, there is probable cause to believe that Boiko facilitated money laundering for a significant cybercriminal known by the online moniker "Moneybooster" by providing Moneybooster with a foreign bank account for the purpose of receiving funds attempted to be stolen from U.S. victims of cybercrime.

13. On or about March 20, 2017, a known cybercriminal known as "Moneybooster" had a chat with gangass@exploit.im. Moneybooster asked "gangass" for a corporate account that could receive a wire of about "200-300k." Within minutes, gangass responded by providing the following account: (1) Company Name: Arco Technology (Hongkong) Limited; (2) Company Address: Unit 2103, 21/F., Sino Centre, 582-592 Nathan Road, Mongkok, Kowloon; (3) Bank Name: Bank of China (Hong Kong) Limited; (4) Bank Address: 213 Queens Road East, Wan Chai, Hong Kong; (5) Account no: 012-899-0-800722-9 (USD). After receiving the information, the cybercriminal informed gangass that "I've sent around 300k." Gangass responded, "[g]ot you, bro!"

14. Several days later, the cybercriminal informed gangass that the transfer was blocked and did not go through. In response, gangass stated, "well, anyway, I already knew it didn't work out. The main thing, do you think the credentials are compromised

or we can keep using them." Moneybooster wrote, in part, "it won't kill your credentials . . . but the same bank won't work for me because it's on the Chase blacklist." Based on my training and

experience, this conversation shows that gangass was aware that the funds are being obtained from a victim whose bank account login information was stolen and that the attempted transfer was fraudulent. During the same conversation, Gangass told Moneybooster, "I have 1 more for you." Based on my training and experience, this constitutes an offer by Gangass to provide Moneybooster with another cash-out bank account. On March 27, 2017, Gangass wrote to Moneybooster, "OTRv2." Based on my training and experience, "OTR" refers to going "off the record" by switching to encrypted communications.

15. Documents retained by JPMC showed that on the same date as the initial chat above, March 20, 2017, a wire in the amount of $276,300 – the same approximate amount referred to by Moneybooster – was initiated from a victim business entity in California to the exact same account in Hong Kong (722-9) provided by gangass (Boiko). JPMC rejected the wire on suspicion of fraud, and neither the victim business entity nor JPMC suffered any loss.

16. A recent court-authorized search of Boiko's email account amgcls32@gmail.com revealed direct evidence that Boiko controlled the Hong Kong bank (722-9) used in the aforementioned transaction and that he is, in fact, gangass@exploit.im. In his email account, Boiko received an email sent by margaritebymhu@seznam.cz on March 29, 2017. The email included an attachment showing an international transfer application from Bankwest in Australia. The transfer was for approximately 47,000 Australian dollars to Arco Technology LTD, account #012-899-0-800722-9 at Bank of China in Hong Kong. This is the same account sent by gangass to Moneybooster one week prior in the Jabber chats mentioned above. The search also revealed a February 2, 2016 email from Jabber confirming the registration of "gangass@jabber.at," which constitutes further confirmation that Boiko uses the moniker "gangass."

17. Additionally, as explained above, photographs publicly available in Boiko's Instagram account are consistent with his laundering money through Chinese accounts, including the photograph posted on August 25, 2015 that shows a large stack of Chinese Yuan on a table. Underneath the stacks of money is a sign that says "Maksim" and the date of August 25, 2015.

Boiko's Money Laundering Relationship with the QQAAZZ Crime Group

18. The FBI's Pittsburgh Field Office located in the Western District of Pennsylvania has been engaged in an ongoing investigation of the QQAAZZ transnational organized crime group that provides money laundering services to significant cybercriminals. As explained below, there is probable cause to believe that Boiko conspired with the QQAAZZ group to facilitate its money laundering activities. The QQAAZZ group, named after an online criminal moniker used by the organization, has operated since at least 2015 and is comprised of more than a dozen individuals from various countries including Georgia, Bulgaria and Latvia.

Overview of QQAAZZ Crime Group

19. The QQAAZZ group and its members opened and maintained hundreds of bank accounts at financial institutions in numerous countries throughout the world, including the United Kingdom, Portugal, Spain, Germany, Belgium, Turkey and the Netherlands. The QQAAZZ group then utilized the bank accounts to receive and launder money stolen by cybercriminals from unsuspecting victims and their respective financial institutions, including in the Western District of Pennsylvania.

20. QQAAZZ group members opened both personal bank accounts and corporate bank accounts at numerous financial institutions for the sole purpose of using the accounts to receive stolen funds from victims. Compared to personal bank accounts, corporate bank accounts were able to receive larger sums of stolen funds without raising the suspicion of bank officials.

21. To open corporate bank accounts, QQAAZZ members registered dozens of shell companies that conducted no legitimate business activity. Using the corporate registration documents, QQAAZZ members then opened corporate bank accounts in the names of the shell companies at numerous financial institutions within each country. The opening of these corporate accounts, in conjunction with the opening of personal accounts, generated hundreds of QQAAZZ-controlled bank accounts throughout the world.

22. At times, QQAAZZ members registered shell companies and opened bank accounts using their true names and their legitimate identification documents. At other times, QQAAZZ members registered shell companies and opened bank accounts using alias names and fraudulent identification documents.

23. QQAAZZ advertises its cash-out and money laundering services on exclusive, underground, Russian-speaking, online cybercriminal forums, including Mazafaka and Verified. In one post QQAAZZ advertised, "a global, complicit bank drops service." Based on my training, experience and direct participation in the investigation, your Affiant is aware that the QQAAZZ group's advertisement indicates the availability of bank accounts in numerous countries throughout the world with "drops" (i.e., money mules) who are complicit in, and knowledgeable of, the criminal scheme.

24. QQAAZZ communicated with its cybercriminal clientele using Jabber, a secure online instant messaging software. QQAAZZ's online monikers included, but were not limited to, "qqaazz," "globalqqaazz," "markdevido," "richrich," "donaldtrump55," "manuel," "krakadil," "kalilinux," "ritchie," "totala," "totala22" and "salazar001."

25. The QQAAZZ group's cybercriminal clientele typically have access to groups of malware-infected computers, also known as "botnets." Once a computer is infected with malware,

the cybercriminals then capture the victim's online banking credentials. The cybercriminals then use the victim's credentials to log into the victim's bank account and initiate fraudulent wire transfers to accounts controlled by the subjects. The QQAAZZ group and the cybercriminal (i.e., botnet owner[1]) then agree on a percentage split from the illicit proceeds stolen from victim bank accounts.

26. QQAAZZ's service generally operated in the following manner:

(a) cybercriminals with unauthorized access to a victim's bank account contacted QQAAZZ via Jabber, a secure online instant messaging software, seeking a recipient bank account to which the cybercriminal could send the victim's stolen funds via electronic funds transfer;

(b) QQAAZZ provided the cybercriminal with the details of the specific bank account designated to receive the stolen funds;

(c) the cybercriminal initiated, or attempted to initiate, an electronic funds transfer from the victim's bank account to the recipient account provided and controlled by QQAAZZ;

(d) QQAAZZ received the stolen funds in its recipient bank account;

(e) QQAAZZ withdrew (i.e., "cashed-out") the funds, transferred the funds to other QQAAZZ-controlled bank accounts for withdrawal, or transferred the funds to illicit "tumbling" services where the funds were converted to cryptocurrency;

(f) QQAAZZ returned the stolen funds to the cybercriminal minus QQAAZZ's fee, which was typically between 40 to 50 percent of the total amount of stolen funds.

[1] The term "botnet owner" is used for simplicity. In reality, the botnet owner, like QQAAZZ, is often a group of people working together to infect victims with malware and steal money from their bank accounts.

27. Because the QQAAZZ group provides its services to numerous nefarious cybercriminal malware organizations, it has been able to facilitate the theft of an estimated tens of millions of dollars from victims in the United States and throughout the world.

Boiko's Close, Personal Relationship with a QQAAZZ Leader

28. As explained below, an individual referred to herein a "Conspirator A" is one of the leaders of the QQAAZZ group.

29. A court-authorized search of Boiko's Apple iCloud account associated with Boiko's email amgcls32@gmail.com in March 2020 revealed several personal photos of Conspirator A.

30. A federal search warrant was issued on February 19, 2020, in the Western District of Pennsylvania for an Apple iCloud account controlled by a member of the QQAAZZ group. Saved in the account was a chat between Conspirator A and the other QQAAZZ group member in which they reference the name "Boiko Maksim Sergeyevich," his location, Saint Petersburg, and the Russian phone number +79817350504[2]. As explained below, +79817350504 is a phone number controlled by Boiko. This further establishes Boiko's connection with the leaders of the QQAAZZ organization.

Search of QQAAZZ Controlled Email and Cloud Storage Account

31. On March 22, 2019, a search warrant was issued in the Western District of Pennsylvania for a QQAAZZ-controlled email account. A review of the account's Google Drive content showed that the users of the saved several documents and folders to their Google drive.

[2] As detailed herein, this Russian phone number belongs to Maksim Boiko.

Three folders were saved as "BG," "ES," and "PT" and contained information related to QQAAZZ controlled shell companies and bank accounts located in Bulgaria, Spain and Portugal.

32. The account contained a directory (arranged by country) listing the names of dozens of shell companies, the purported owner/director of each shell company, the owner's contact information, and details for dozens of bank accounts opened in each shell company's name at multiple financial institutions.

33. One of the folders in the account was marked "PT" for Portugal. The folder contained more than thirty (30) subfolders each designated by the name of a different Portuguese shell company. Portuguese authorities confirmed that the shell companies listed in the "PT" folder were registered in Portugal and that they conducted no legitimate business. Within each subfolder was the name and contact information of the owner/director of the shell company, along with the details for dozens of bank accounts opened in the names of the shell companies at dozens of different Portuguese banks. Portuguese authorities further confirmed that the bank accounts listed within the "PT" folder were used solely for the criminal purposes described below. According to Portuguese authorities, in order to open corporate bank accounts in Portugal, the purported director/owner of the company must go into the bank branch and provide identification documents.

34. Numerous identified members of the QQAAZZ conspiracy, including Aleksejs Trofimovics referenced below, used both legitimate and fraudulent identification documents to register the Portuguese shell companies and/or opened the Portuguese bank accounts. More significantly, these bank accounts received, or were intended to receive[3], funds stolen from victims

[3] Some of the attempted electronic funds transfers intended for the QQAAZZ-controlled beneficiary bank accounts were stopped by the banks when fraud was detected.

of cybercrimes on behalf of the QQAAZZ group. In fact, the investigation confirmed that twenty (20) of these Portuguese bank accounts either received, or were designated to receive, unauthorized electronic funds transfers from the bank accounts of U.S. victims between 2016 to the present.

Fraudulent Transactions Involving U.S. Victims

35. The following table sets forth examples of the stolen funds from U.S. victims that were transferred, or attempted to be transferred, to QQAAZZ beneficiary bank accounts opened and maintained by the QQAAZZ group:

Date:	Victim:	Victim Bank:	Attempted Loss:	Actual Loss:	Beneficiary Bank Account:
3/7/17	PMS	Schwab	$75,000.00	$44.30	Banco Comercial Portugues Account ending 8205 Aktrofi Services LDA
9/20/17	JBK	BOA	$84,900.00	$0.00	Bankinter S.A. Account ending 4628 Aktrofi Services LDA
10/26/17	CYL	JP Morgan Chase	$98,780.00	$0.00	Bankinter S.A. Account ending 0343 Privelegioasis LDA
11/29/17	A&DG	American Express	$121,360.00	$64,082.69	Caixa Economica Montepio Geral Account ending 3596 Selbevulte LDA
11/30/17	HSW&MS	BB&T	$72,000.00	$0.00	Bankinter S.A. Account ending 0343 Privelegioasis LDA
3/8/18	LC	USAA	$29,500.00	$29,500.00	Caixa Economica Montepio Geral Account ending 3197

					Flamingocloud LDA
3/8/18	LC	USAA	$29,500.00	$0.00	Caixa Economica Montepio Geral Account ending 9543 Colossal Devotion LDA
3/21/18	M US	BOA	$49,000.00	$0.00	Caixa Economica Montepio Geral Account ending 9543 Colossal Devotion LDA
4/10/18	PES	JP Morgan Chase	$59,426.28	$0.00	Caixa Geral de Depositos Account ending 3078 Cardinal Gradual LDA
4/10/18	WES	JP Morgan Chase	$59,426.28	$0.00	Caixa Geral de Depositos Account ending 3078 Cardinal Gradual LDA
4/10/18	CDW	JP Morgan Chase	$59,426.28	$0.00	Caixa Geral de Depositos Account ending 3078 Cardinal Gradual LDA
8/30/18	YC	PNC (Western District of PA)	$99,693.36	$0.00	Banco BPI S.A. Account ending 0175 Selbevulte LDA
11/14/18	GSSS	BOA	$56,202.25	$56,202.25	Best-Banco Electronico de Servico Total S.A. Account ending 1884 Aktrofi Services LDA
11/14/18	GSSS	BOA	$112,921.23	$112,921.23	Banco Activobank S.A. Account ending 9194 Deinis Gorenko
11/14/18	GSSS	BOA	$45,830.77	$45,830.77	Banco CTT S.A. Account ending 2490 Deinis Gorenko
12/6/18	KM	JP Morgan Chase	$114,652.61	$114,652.61	Bankinter S.A. Account ending 1304

					Flamingocloud LDA

Additional QQAAZZ Activity Relating to the Western District of Pennsylvania

37. In addition to the initiation of unauthorized electronic funds transfers from PNC Bank in the Western District of Pennsylvania, a similar unauthorized electronic funds transfer was initiated from First National Bank in the Western District of Pennsylvania.

38. QQAAZZ's cybercriminal clientele include a known cybercriminal who was recently prosecuted in the Western District of Pennsylvania. The known cybercriminal and QQAAZZ engaged in extensive Jabber chat communications in furtherance of their cybercriminal schemes. A search of the known cybercriminal's computer revealed saved Jabber chat communications with QQAAZZ dating back to early 2015. During a particular chat on February 18, 2016, QQAAZZ provided the cybercriminal with a bank account in the name Yaromu Gida Ltd., at a bank located in Bursa, Turkey, for the purpose of sending stolen victim funds to the account.

39. Significantly, in March 2016, an attempt was made to steal over $100,000 from a victim's bank account in the U.S., with the money destined for the same account in the name Yaromu Gida Ltd. In Turkey sent from QQAAZZ to the known cybercriminal.

40. Additionally, on April 7, 2016, First National Bank of Pennsylvania ("FNB"), located in the Western District of Pennsylvania, was contacted by a corporate client regarding suspicious activity detected in the client's business checking account. FNB reviewed the customer's account and observed that an unauthorized international wire was pending approval for $176,500, destined for a beneficiary account in the same name of Yaromu Gida Ltd., located in Bursa, Turkey.

QQAAZZ's Jabber Communications and "Atrofi95" Bitcoin Wallet

41. As part of its investigation, the FBI obtained communications between QQAAZZ and numerous cybercriminal clients.

42. On November 14, 2016, qqaazz@mazafaka.info, a known Jabber account used by the QQAAZZ group, discussed purchasing corporate drop accounts from a cybercriminal and requested the cybercriminal's Bitcoin wallet to pay for the drop accounts. Next, qqaazz@mazafaka.info sent confirmation that qqaazz paid the cybercriminal from his Bitcoin wallet "Atrofi95."

43. Additionally, during intercepted Jabber chats on December 19, 2016, globalqqaazz@exploit.im, another known Jabber account used by the QQAAZZ group, and another cybercriminal discussed the sale of three hundred credit cards. Once globalqqaazz@exploit.im agreed to purchase the cards, he sent the cybercriminal confirmation of a Bitcoin transaction from the same aforementioned "Atrofi95" wallet sent by qqaazz@mazafaka.info on November 14, 2016. This provides further evidence that the online monikers qqaazz@mazafaka.info and globalqqaazz@exploit.im are controlled by the same individual or group of individuals within the QQAAZZ group. More significantly, this provides evidence that the QQAAZZ group uses a Bitcoin wallet in the name "Atrofi95" in furtherance of its criminal activities.

44. A search of FBI databases revealed records of an account with BTC-e for "Atrofi95," the name of the Bitcoin wallet passed by the QQAAZZ group in the chats described above. BTC-e was a cryptocurrency trading platform frequently used by cybercriminals until the U.S. government seized their website. The BTC-e website went offline on July 25, 2017, following

the arrest of BTC-e staff members and the seizure of server equipment at one of their data centers.[4] This BTC-e account was registered to Aleksejs Trofimovics in London with the corresponding email address atrofi95@gmail.com. It should be noted that, for his role in the QQAAZZ money laundering conspiracy, Aleksejs Trofimovics was arrested in Latvia in October 2019 and extradited to the United States in early 2020 to face prosecution in the Western District of Pennsylvania.

45. On January 18, 2019, United States Magistrate Judge Robert C. Mitchell signed a search warrant for two email accounts including atrofi95@gmail.com. Google responded on January 21, 2019. The results showed the email account atrofi95@gmail.com had been recently accessed from numerous U.K.-based IP addresses and was registered with U.K. phone number +447575761176.

46. Email content contained in the return showed the atrofi95@gmail.com account received emails from currency exchange platforms such as Coinbase, Bitstamp and Revolut, indicating atrofi95@gmail.com was used to register accounts with all of these platforms. One email confirmed the Revolut account registered with the atrofi95@gmail.com sent 10,000 British pounds to a bank account in Germany on November 8, 2018. This is consistent with the e-mail account atrofi95@gmail.com being used by the QQAAZZ group to facilitate money laundering and other criminal activity through online currency exchangers, similar to what was done by QQAAZZ via BTC-e, as described above.

47. On January 25, 2019, the Bitcoin exchange company Bitstamp provided records for a Bitstamp account in the username "atrofi95." The Bitstamp records verified the account was in

---

[4] *See* https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged

the name Aleksejs Trofimovics and was registered with the email account atrofi95@gmail.com and phone number +447575761176, the same phone number used to register the email account atrofi95@gmail.com.

Search of QQAAZZ Apple iCloud Account Associated with atrofi95@gmail.com

48. On March 8, 2019, a United States Magistrate Judge in the Western District of Pennsylvania signed a search warrant for the Apple iCloud account registered with email account atrofi95@gmail.com. The information contained in this iCloud account provided substantial leads in the Western District of Pennsylvania investigation.

49. The return from Apple showed that account registered with atrofi95@gmail.com listed the subscriber name as Aleksejs Trofimovics with contact number +447575761176, which is consistent with the returns described above from Google and Bitstamp. However, included in the return from Apple were also records from the account's iCloud Drive (storage).

50. Found within the account was a list of QQAAZZ's usernames and hashed passwords for various websites used in furtherance of the group's criminal scheme. For example, the group's username to access the aforementioned Mazafaka site on which the group advertised its criminal services was listed as "qqaazz." Additionally, screenshots found within the cloud storage account showed the user controlling and utilizing several online monikers, such as globalqqaazz@exploit.im, used by QQAAZZ to communicate with its cybercriminal clientele over a secure instant messaging platform.

51. The iCloud drive also contained a folder for items saved to the iCloud account from WhatsApp. Specifically, this folder contained communications exchanged via WhatsApp with the U.K. phone number +447535982576 (hereinafter X2576). While the WhatsApp chats were

encrypted, media sent between X2576 and other WhatsApp numbers, such as videos, pictures, documents, etc., were not encrypted and were stored in the atrofi95@gmail.com iCloud account.

52. The X2576 WhatsApp account exchanged information with other WhatsApp numbers directly pertaining to the activities of the QQAAZZ group. For example, several folders in the iCloud drive contained screenshots of Jabber chats with known QQAAZZ Jabber accounts donaldtrump55@exploit.im, markdevido@exploit.im, and others.

53. The evidence from the iCloud return also confirmed that the QQAAZZ group creates and utilizes fake identification and registration cards in several countries, including the U.K. For example, the media passed between the X2576 phone number and phone number +447398469445 via WhatsApp contained screenshots depicting materials used to create fake U.K. identification documents.

54. The information found in the atrofi95@gmail.com iCloud return gives the FBI probable cause to believe that U.K. phone number X2576 was a criminally controlled account utilized in furtherance of the QQAAZZ group's illicit activities. Indeed, the communications saved between X2576 and other WhatsApp numbers appeared to be entirely, or almost entirely criminal in nature.

Criminal Communications Between X2576 and Boiko's Russian Phone Numbers

55. A review of the atrofi95@gmail.com iCloud contents revealed two Russian WhatsApp numbers that exchanged information associated with QQAAZZ's money laundering scheme with the QQAAZZ phone number X2576: these numbers were +79817350504 (hereinafter X0504) and +79531782920 (hereinafter X2920). As explained immediately below, both of these phone numbers were controlled by Maksim Boiko.

56. In response to legal process, Google provided the FBI with subscriber information for the email account plinofficial@gmail.com. The account was registered in the name Maxim Boiko with registration phone number X0504, the same number as in the WhatsApp chats found in the atrofi95 iCloud account. The recovery email was listed as plinofficial@me.com.

57. In response to legal process, Google provided the FBI with subscriber information for the Facebook account registered with the email account plinofficial@gmail.com**.** The account was registered in the name Maxim Boiko with registration cell phone X0504, the same number as in the WhatsApp chats found in the atrofi95 iCloud account.

58. Additionally, in a U.S. visa application from February 2018, Boiko listed his phone number as +79817350504 (X0504). Accordingly, there is probable cause to believe Maksim Boiko controls phone number X0504.

59. In response to legal process, Apple provided subscriber information about the email account amgcls32@icloud.com. The results showed that the account was registered with the email account amgcls32@gmail.com and registration phone number X2920, the other Russian phone number that was in communication with X2576 in the atrofi95@gmail.com iCloud account.

60. On March 25, 2020, Google responded to a search warrant signed in the Western District of Pennsylvania for the email account amgcls32@gmail.com. Numerous documents found in the email account, including Boiko's passport, confirm that the account was controlled by Boiko. Because the X2920 phone number was used to register for an iCloud account tied to the email address amgcls32@gmail.com, there is probable cause to believe Maksim Boiko controls phone number X2920.

61. A review of the communications with X0504 revealed several incriminating pieces of media used in furtherance of the QQAAZZ money laundering scheme exchanged between the

two numbers. For example, one of the screenshots exchanged between the numbers showed detailed bank account information for the following two QQAAZZ-controlled shell companies registered in Portugal whose corporate bank accounts received, or were intended to receive stolen funds from U.S. victims. Those shell companies were: Sauvage Real LDA and Privilegioasis LDA.

62. As explained above, on March 22, 2019, a search warrant was issued in the Western District of Pennsylvania for a QQAAZZ-controlled email account containing specific details associated with QQAAZZ controlled shell companies and bank accounts located in Bulgaria, Spain and Portugal.

63. Among the many shell companies listed in the folder were Sauvage Real, LDA and Privilegioasis, LDA, the same two companies mentioned in the screenshot between X2576 and Boiko's number, X0504.

64. The FBI has located numerous fraudulent wire transfers sent, and attempted to be sent, to Sauvage Real, LDA from U.S. companies. For example, on August 30, 2018, PNC Bank in Pittsburgh, Pennsylvania, reported three fraudulent wire transfers totaling nearly $700,000 from a U.S. victim company located in Ohio. One of three fraudulent wires was initiated in the amount $498,536.36 for an account in the name Sauvage Real LDA at Banco de Investimento in Portugal. PNC Bank was able to stop this wire and did not suffer a loss.

65. Bank records from JP Morgan Chase showed that on November 9, 2017, a $98,700 fraudulent wire transfer was initiated from a Skokie, Illinois business bank account with JP Morgan Chase Bank. This wire transfer was intended for an account in the name a Sauvage Real LDA at Bankinter in Portugal. The account number on Sauvage Real's Bankinter account (ending in 6079)

was identical to the account number sent in the screenshot between X2576 and X0504. JP Morgan Chase was able to recover the funds and did not suffer a loss.

66. Furthermore, the other Portuguese company and bank account mentioned in the screenshot exchanged with Boiko's WhatsApp number was *also* the intended recipient of fraudulently obtained funds from U.S. victims. For example, on October 26, 2017, a fraudulent wire in the amount of $98,780 was initiated from a New York based religious institution's Chase bank account to Privilegioasis' Bankinter account (ending in 0343). This is the same bank account number sent in the WhatsApp chat between X2576 and X0504. JPMC was able to stop the wire before it left the bank and suffered no loss.

67. Another exchange between the X2576 and X0504 WhatsApp numbers showed an image taken on October 24, 2017 of chats on a phone where one party says, "[h]oly shit you did, you transferred it. You're like a wizard." The same party then states, "Bro, if it isn't too much of a bother, please ask about this login – Atrofi95. A wire was sent to BTC-e on July 22nd for 45k. The other party in the chat then mentions the company Mayzus Financial and states, "[g]otta contact Moneypolo.[5]" As discussed above, the QQAAZZ group used the Atrofi95 BTC-e account to launder criminally obtained funds.

68. In addition to criminal communications between X2576 and Boiko's number X0504, a review of the iCloud's contents also showed incriminating media sent between X2576 and the second Russian phone number belonging to Boiko, X2920. For example, in one of the screenshots sent between the two numbers, a Gmail account is open and visible in the background.

---

[5] MoneyPolo was a subsidiary of Mayzus Financial Services and Mayzus Financial Services had significant financial ties to BTC-e. *See* https://blog.moneypolo.com/en/official-statement-by-senior-management-of-mayzus-financial-services-ltd-with-regards-to-closure-of-btc-e-com-exchange-service/.

One of the emails in the background states, "[d]ear [Conspirator A] …" As discussed above, Conspirator A has been charged with conspiracy to commit money laundering out of the Western District of Pennsylvania stemming for his involvement with the QQAAZZ group. Boiko's X2920 number and the QQAAZZ controlled X2576 number also exchange screenshots of balances in various cryptocurrency accounts, confirmations of cryptocurrency payments, and other similar information.

69. In a screenshot sent between the X2576 and the X2920 phone numbers, there is an image displayed that states "user detail" and lists the user as "amgcls32" and associated phone number as X2920. Additional screenshots exchanged between the X2576 and X2920 phone numbers contain information about Bitcoin transactions and confirmations. The X2920 number was saved in the contact list for criminally controlled QQAAZZ email account atrofi95@gmail.com as "Maximile."

70. Several screenshots exchanged between the X2576 and the X2920 numbers also show an open Mac laptop computer with the name "Max" assigned to the computer. The images on the computer showed confirmations of Bitcoin transactions and similar information. Therefore, there is probable cause to believe that the computer "Max" belongs to Maksim Boiko and that Boiko is using his laptop computer in furtherance of money laundering activities.

71. Because Conspirator A and the QQAAZZ group used phone number X2576 as a criminally controlled number in furtherance of the groups' cybercriminal activity, and exchanged criminally controlled bank accounts and other similar information with Russian WhatsApp numbers X0504 and X2920 controlled by Boiko, the FBI has probable cause to believe that Boiko was assisting and facilitating Conspirator A and the QQAAZZ group launder money stolen from victims located in the U.S. and elsewhere.

Emails Connecting Boiko to QQAAZZ Group Criminal Activity

72. Bank records and interviews with a Connecticut-based victim showed that a bank account in Spain was the intended recipient of funds attempted to be stolen from the victim's bank account in late 2016. On October 7, 2016, Banco Santander S.A. bank account ES2000494738112916142172 in the business name STEFILAZ S.L. was the intended recipient of a $198,435.70 fraudulent wire transfer from a U.S. victim company in Windsor, Connecticut. Additionally, on November 8, 2016, Banco Santander S.A. bank account ES2000494738112916142172 in the business name STEFILAZ S.L., was the intended recipient of a $48,000 fraudulent wire transfer from a U.S. victim company in Montclair, New Jersey. This bank account in the name STEFILAZ S.L., opened in the name Stefan Trifonov Zhelyazkov, was the intended recipient of money wired from U.S. victims stolen as a result of computer intrusions and bank account takeovers.

73. As discussed above, on March 22, 2019, a search warrant was issued in the Western District of Pennsylvania for a QQAAZZ controlled email account contained criminally controlled QQAAZZ shell companies and bank accounts in Bulgaria, Spain and Portugal.

74. One of the folders in the account was marked "ES" for Spain. The folder contained eight subfolders each designated by the name of a known QQAAZZ group member or alias as well as a shell company in Spain, "STEFILAZ SL." Saved in the "STEFILAZ S.L." sub-folder were two documents titled "DETAILS" and "SANTANDER." The "Details" document contained the following information for business STEFILAZ S.L: Director Stefan Trifonov Zhelyazkov as well as an NIE Number, a CIF Number and an address in Cantabria, Barcelona, Spain. The "Santander" document contained the bank account information for a business and a personal bank account. The

account number for the business bank account was ES2000494738112916142172. This is the same bank account to which funds stolen from U.S. victims were intended.

75. Also saved in the "ES" folder was a document titled "Copy of Public Deed of Incorporation." This document contained the incorporation documents for STEFILAZ S.L. in Cantabria, Barcelona, Spain. The document listed Stefan Trifonov Zhelyazkov, date of birth (DOB) April 24, 1990, Bulgarian passport number 382081221 and Spanish tax identification number (NIE) Y-4500538-G as the Director of STEFILAZ, SOCIEDAD LIMITADA (STEFILAZ S.L.). The document also contained the Spanish NIF/CIF certification for STEFILAZ S.L. which allowed the company to conduct financial transactions in Spain. Lastly, the document contained a copy of Zhelyazkov's Bulgarian passport that listed the same DOB and passport information mentioned above.[6]

76. As discussed above, on March 25, 2020, Google responded to a search warrant signed in the Western District of Pennsylvania for Boiko's email account amgcls32@gmail.com. A review of the account yielded an email sent on September 2, 2016 from atrofi95@gmail.com, a known QQAAZZ group-controlled email account, to the amgcls32@gmail.com account. Attached to the email was the same Public Deed of Incorporation for STEFILAZ S.L. discussed above. The Certificate of Registration for STEFILAZ S.L. was also attached to the email. Significantly, these documents were sent to Boiko only a month before the first fraudulent wire transfer to STEFILAZ S.L. from the U.S. victim company in Windsor, Connecticut.

[6] Law enforcement authorities confirmed that this passport was fraudulent.

Search of Boiko's Apple iCloud Account and Facilitation of QQAAZZ Money Laundering

77. On March 26, 2020, pursuant to a search warrant issued in this District, the FBI received from Apple the contents of an iCloud account belonging to Boiko and registered with the email address amgcls32@gmail.com. The account contains hundreds of photographs of Boiko, as well as several of Boiko's government identification documents, which demonstrate that Boiko unquestionably controls this account.

78. A review of the iCloud content revealed photographs showing communications over criminally controlled Jabber accounts. For example, one screenshot shows an open Jabber conversation with the moniker salazar001@xmpp.jp. The FBI's investigation has revealed salazar001@xmpp.jp to be a criminally controlled QQAAZZ Jabber account. In the conversation, salazar001@xmpp.jp receives confirmation of payment sent in the amount of 3.482 Bitcoin. The date of this photograph is July 24, 2019. Open source information shows that a transfer of 3.482 Bitcoin was, in fact, made in the amount of 3.482 Bitcoin on July 24, 2019. At this time, 3.482 Bitcoin was equal to approximately $35,000.

79. Also on July 24, 2019, Boiko's amgcls32@gmail.com email account received an email message from Binance. (Binance is a global cryptocurrency exchange that provides a platform for trading more than 100 cryptocurrencies.) The message was sent to firm that Boiko wanted to withdraw and send 3.482 Bitcoin to address 1EuGpYbEfvicrppSpStdxw1bpHsokpP4x. This is the same Bitcoin wallet address provided in the photograph discussed above to which the 3.482 Bitcoin was to be sent.

80. Because this screenshot was located on an iCloud account belonging to Boiko, and Salazar001@xmpp.jp is a Jabber account known by the FBI to be used by the QQAAZZ group in

furtherance of criminal activity, the FBI has probable cause to believe that Boiko was engaged in money laundering activities with the criminally controlled QQAAZZ account.

81. Accordingly, based on the foregoing, your Affiant submits there is probable cause to believe that from in and around 2015 and continuing to the present,

CONCLUSION

82. Based on the above information, your Affiant has probable cause to believe that from in or around 2015, the exact date being unknown, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendant Maksim BOIKO did knowingly and intentionally conspire and agree with other persons known and unknown, to commit money laundering in violation of Title 18, United States Code, Section 1956(h). Accordingly, the United States respectfully requests that a warrant be issued for the arrest of Maksim BOIKO.

The above information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

s/Samantha Shelnick
SAMANTHA SHELNICK
Special Agent, FBI

Special Agent Shelnick attested to this Affidavit by telephone pursuant to FRCP 4.1(b)(2)(A) this 27th day of March 2020

HONORABLE LISA PUPO LENIHAN
United States Magistrate Judge